Malware

Toomas Lepik
course-malware@cert.ee

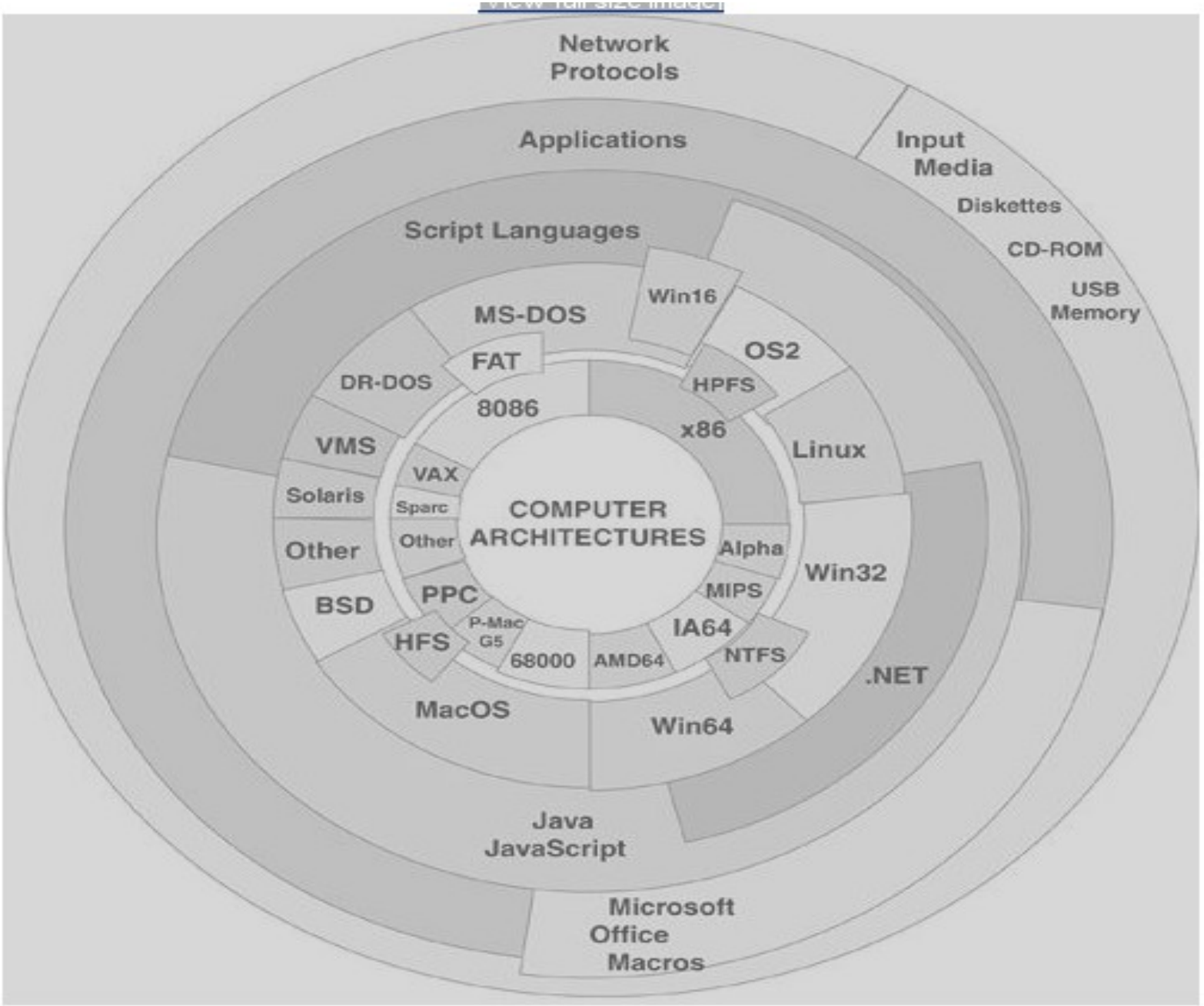
6 sept. 2010

Quick recap

Why they create malware

Operation system usage trends

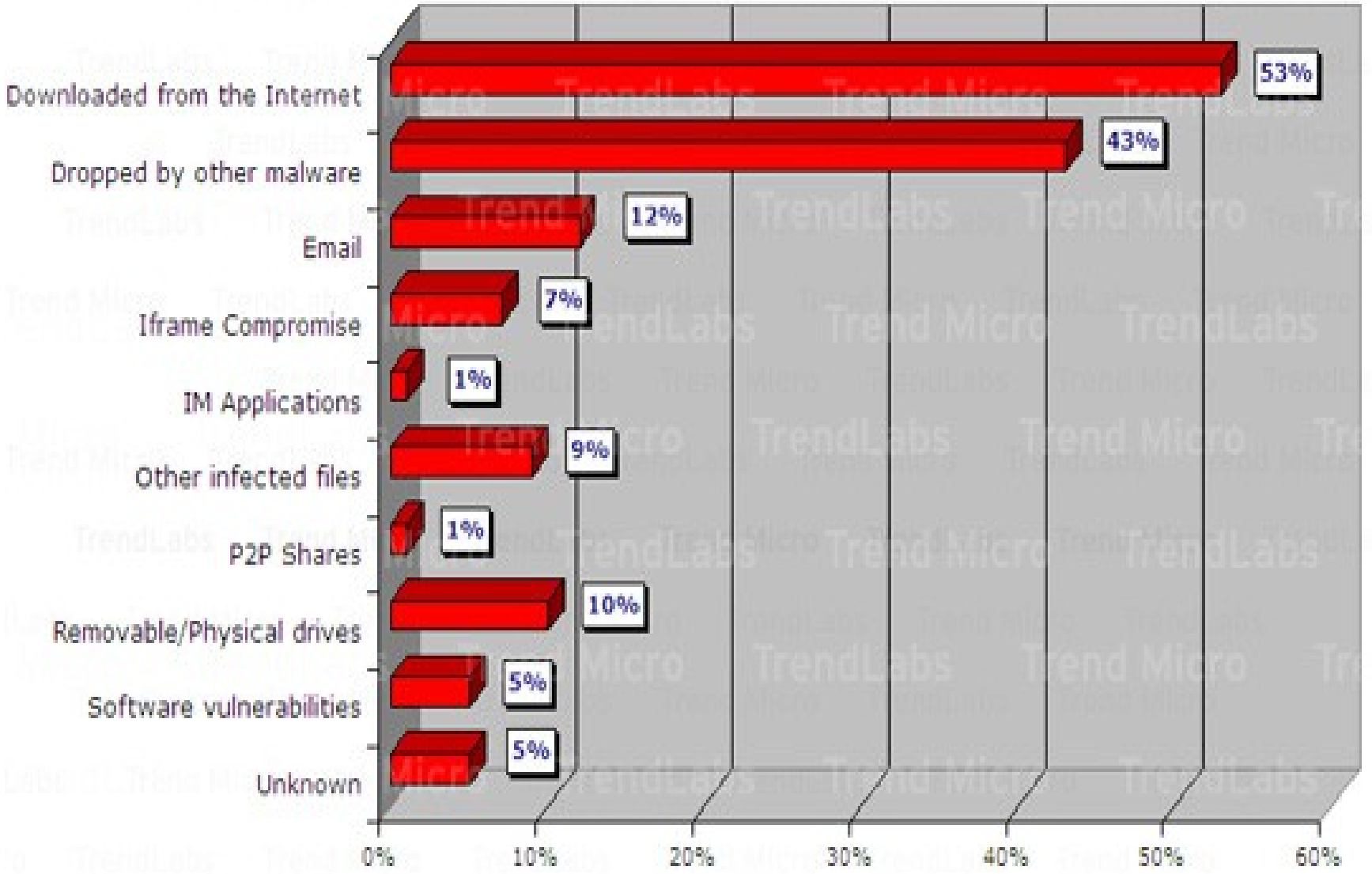
http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10


Network Protocols
Applications
Input Media
Diskettes
CD-ROM
USB Memory
Script Languages
MS-DOS
Win16
OS2
FAT
HPFS
DR-DOS
8086
x86
Linux
VMS
VAX
Solaris
Sparc
COMPUTER ARCHITECTURES
Other
Other
Alpha
Win32
MIPS
PPC
BSD
P-Mac G5
IA64
HFS
68000
AMD64
NTFS
.NET
MacOS
Win64
Java JavaScript
Microsoft Office Macros

How it infects

Vectors

- social engineering
- exploiting unpatched security holes
- Clickjacking
- Thumb drives
- Backups



Coverage: Malware Analyzed by Trend Micro Researchers
Date Range: January 1, 2008 to November 25, 200

Malware
do not call wolf wolf

Viruses

Virus is code that recursively replicates a possibly evolved copy of itself. Viruses infect a host file or system area, or they simply modify a reference to such objects to take control and then multiply again to form new generations.

Worms

Worms = network virus

Usually a worm will execute itself automatically on a remote machine without any extra help from a user.

- Mailers and Mass-Mailer Worms
- Octopus
- Rabbits

Logic Bombs

A logic bomb is a programmed malfunction of a legitimate application. An application, for example, might delete itself from the disk after a couple of runs as a copy protection scheme; a programmer might want to include some extra code to perform a malicious action on certain systems when the application is used. These scenarios are realistic when dealing with large projects driven by limited code-reviews.

Trojan

software may appear to be a legitimate software package that accomplishesa task desired by the user. However, in installing the software, it also performs some illegitimate task at the same time.

- Backdoors
- Password-Stealing Trojans

Germs

Germs are first-generation viruses in a form that the virus cannot generate to its usual infection processes.

Exploits

Exploit code is specific to a single vulnerability or set of vulnerabilities. Its goal is to run a program on a (possibly remote, networked) system automatically or provide some other form of more highly privileged access to the target system.

Downloaders

A downloader is yet another malicious program that installs a set of other items on a machine that is under attack. Usually, a downloader is sent in e-mail, and when it is executed (sometimes aided with the help of an exploit), it downloads malicious content from a Web site or other location and then extracts and runs its content.

Dialers

Program that usually abuses modem connection

Droppers

"installer"

- Injectors
  - Injectors are special kinds of droppers that usually install virus code in memory

Auto-Rooters

Auto-rooters are usually malicious hacker tools used to break into new machines remotely. Auto-rooters typically use a collection of exploits that they execute against a specified target to "gain root" on the machine

Spammer Programm

Spammer programs are used to send unsolicited messages to Instant Messaging groups, newsgroups, or any other kind of mobile device in forms of e-mail or cell phone SMS messages.

- Mass Mailers

Flooder

Program component that can produce network traffic to carry out a denial of service (DoS) attack

Keyloggers

A keylogger captures keystrokes on a compromised system,

Rootkits

Rootkits are a special set of hacker tools that are used after the attacker has broken into a computer system and gained root-level access

Info stealer's

Malware naming scheems

CARO Malware Naming Scheme = Dead
No good alternative

Additional reading
http://www.people.frisk-software.com/~bontchev/papers/naming.html

How to create modern malware

http://www.youtube.com/watch?v=yVL34RpjOWc